# SECURING KEY ACCOUNTS AND DEVICES

## Securing Your Home Network

**A protected home network means your family can use the internet more safely and securely.**

Most households now run networks of devices linked to the internet, including computers, gaming systems, TVs, tablets, smartphones and wearable devices that access wireless networks. To protect your home network and your family, you need to have the right tools in place and confidence that family members can use the internet more safely and securely.

The first step is to keep a clean machine and make sure all of your internet-enabled devices have the latest operating system, web browsers and security software. This includes mobile devices that access your wireless network.

### Secure Your Wireless Router

A wireless network means connecting an internet access point – such as a cable or DSL modem – to a wireless router. Going wireless is a convenient way to allow multiple devices to connect to the internet from different areas of your home. However, unless you secure your router, you're vulnerable to people accessing information on your computer, using your internet service for free and potentially using your network to commit cybercrimes.

### Here are ways to secure your wireless router:

- **Change the name of your router:** The default ID – called a service set identifier" (SSID) or "extended service set identifier" (ESSID ) – is assigned by the manufacturer. Change your router to a name that is unique to you and won't be easily guessed by others.
- **Change the preset password on your router:** Leaving a default password unchanged makes it much easier for hackers to access your network. You should change it as soon as possible. A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, "I love country music."). On many sites, you can even use spaces!
- **Review security options:** When choosing your router's level of security, opt for WPA2, if available, or WPA – these levels are more secure than the WEP option.

- **Create a guest password:** Some routers allow for guests to use networks via separate guest passwords. If you have many visitors to your home, it's a good idea to set up a guest network.
- **Use a firewall:** Firewalls help keep hackers from using your device to send out your personal information without your permission. While antivirus software scans incoming email and files, a firewall is like a guard, watching for attempts to access your system and blocking communications with sources you don't permit. Your operating system and/or security software likely comes with a pre-installed firewall, but make sure you turn on these features.

### Protect yourself with these STOP. THINK. CONNECT.™ tips:

- **Keep security software current:** Having the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats.
- **Protect all devices that connect to the internet:** Along with computers, smartphones, gaming systems and other web-enabled devices also need protection from viruses and malware.
- **Plug & scan:** USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.
- **Protect your $$:** hen banking and shopping, check to be sure the sites is security enabled. Look for web addresses with "https://," which means the site takes extra measures to help secure your information. "http://" is not secure.
- **Back it up:** Protect your valuable work, music, photos and other digital information by making electronic copies of your important files and storing them safely.

Find more information at https://www.staysafeonline.org